

ABSTRACT OF THE DISCLOSURE

Obscuring cryptographic computations may be accomplished by performing modular exponentiation of an exponent in a cryptographic computation such that memory accesses are independent of the exponent bit pattern, thereby deterring timing attacks.